

Wild West of Conference Apps Security

- Yashvier Kosaraju
Twilio

\$Whoami

- Product Security @ Twilio
- ~6 years in Security
- Amateur Photographer
- Love Hiking
- Scared of heights

linkedin.com/in/yashvier/
[@yashvi3r](https://twitter.com/yashvi3r)

DISCLAIMER

- The intention of the talk is not to call anyone out but to raise awareness
- I do not suggest using **OR** not using any of the vendors
- Not releasing the scripts/tools

Agenda

- Motivation
- Hypothesis
- Primary Research
- Testing Process
- Findings
- Responsible Disclosure
- Recommendations
- Open Questions & Future Work
- Q/A



Motivation

- Tested a conference app built by a third party
- Found many many many issues hidden in features like:
 - Find other attendees
 - Messaging features



Motivation

- Then in the news...
- <https://mashable.com/2018/04/20/rsa-app-data-exposed>
- <https://ninja.style/post/bcard/>
 - How I Hacked BlackHat 2018
- <https://www.zdnet.com/article/uk-conservative-party-conference-app-leaks-mps-personal-details/>

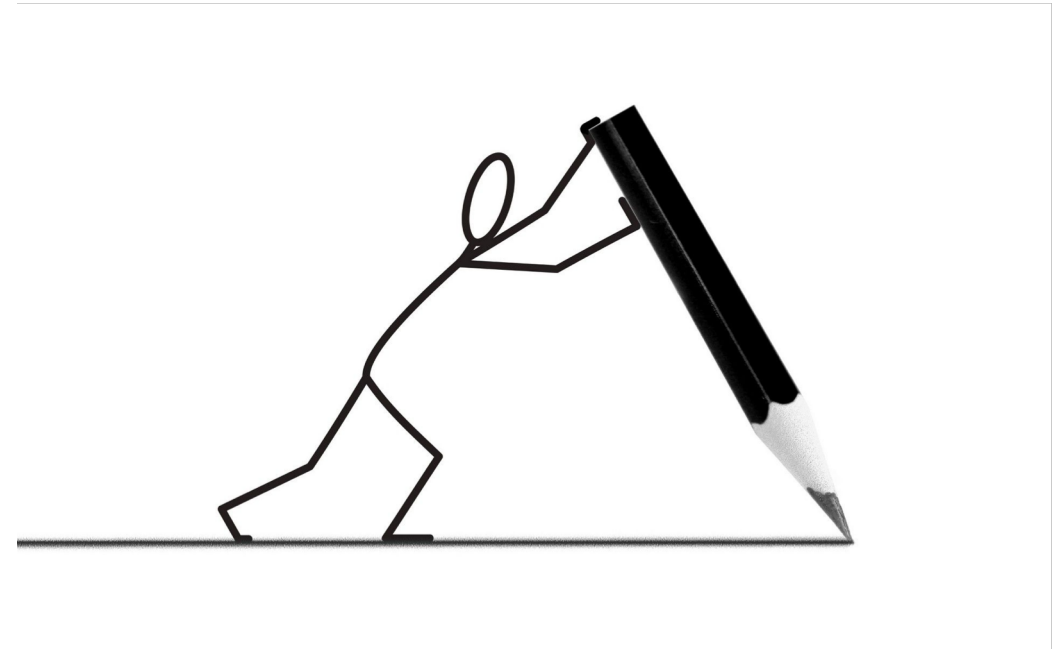
Hypothesis

- Many conference apps are built by third party vendors
- A large amount of data can be extracted from these apps, using inbuilt *features*



Hypothesis

- Boundaries of the research:
 - No exploits
 - No brute force
 - No invasive testing
 - No automated scanning
- Only use 'Features'
- So just "*using*" the apps.....



Primary Research

- What are the typical features conference apps provide?
- What kind of authentication do these apps provide?
- Are any 'features' leaking sensitive data?

Primary Research

- Static apps
 - Just details of event
 - Maps
 - Agenda
 - etc
- Dynamic apps
 - Users can login
 - Create a profile
 - Link accounts
 - Facebook, Twitter, LinkedIn
 - Chat with other attendees

Primary Research

- Some forms of authentication:
 - Username/password
 - Passcode
 - Email verification
 - **Unauthenticated**



Primary Research

- Interesting features:
 - Chat with other attendees
 - Find other attendees
 - List all attendees
 - And more...

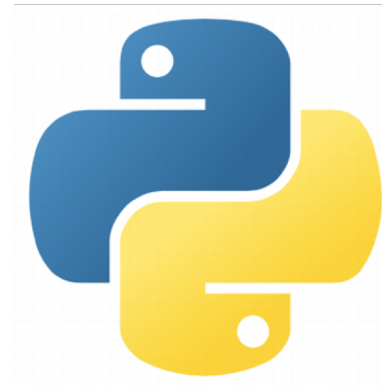


Primary Research

Unauthenticated + List all
attendees

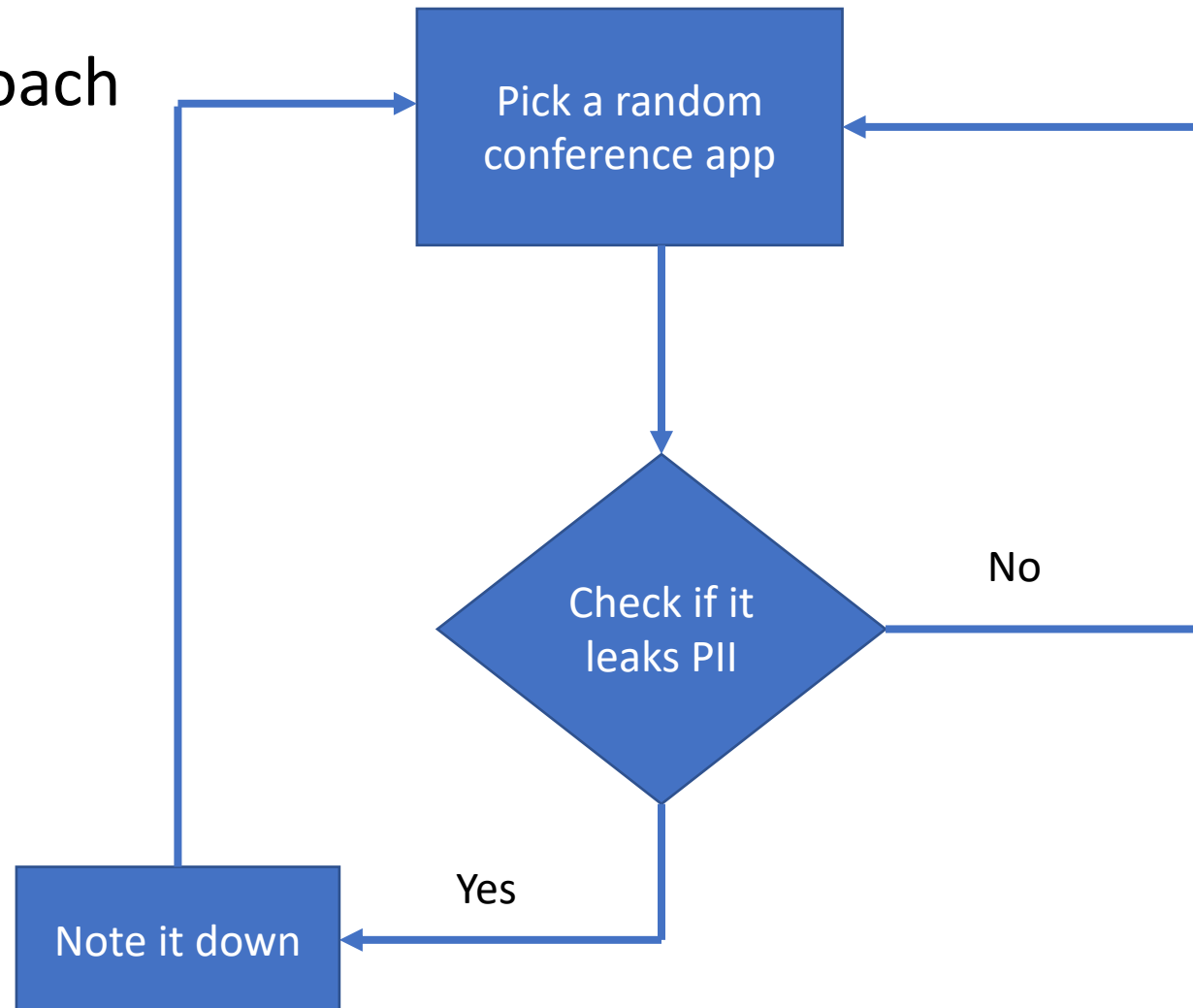
Testing Methodology

- Tools Used:



Testing Methodology

- Initial Approach



Testing Methodology

- Did this for a few apps.
- Then it hit me...

There are many many conference apps

Testing Methodology

- How many conference apps are there??



https://www.quora.com/How-many-conferences-conventions-tradeshows-and-exhibitions-happen-in-

photography useful hacks ISEC learning resources visa docs aws appscan tric

Quora

Home

Answer

Spaces

Notifications ²¹

Search C

 , the conference discovery 
platform
Answered Jun 15, 2016

Nobody knows the answer to this. It depends to a great degree on how you define conventions, tradeshows and exhibitions (and conferences). Best we could guess when we were running conference hound is that there may be up to 1 million individual events every year in the world ranging from the very large to relatively small. There are so many and the industry is so disaggregated that aggregating and counting them is actually a more than trivial problem to solve.

3.9k Views · View Upvoters

 Upvote · 3  Share



Add a comment...

Recommended All

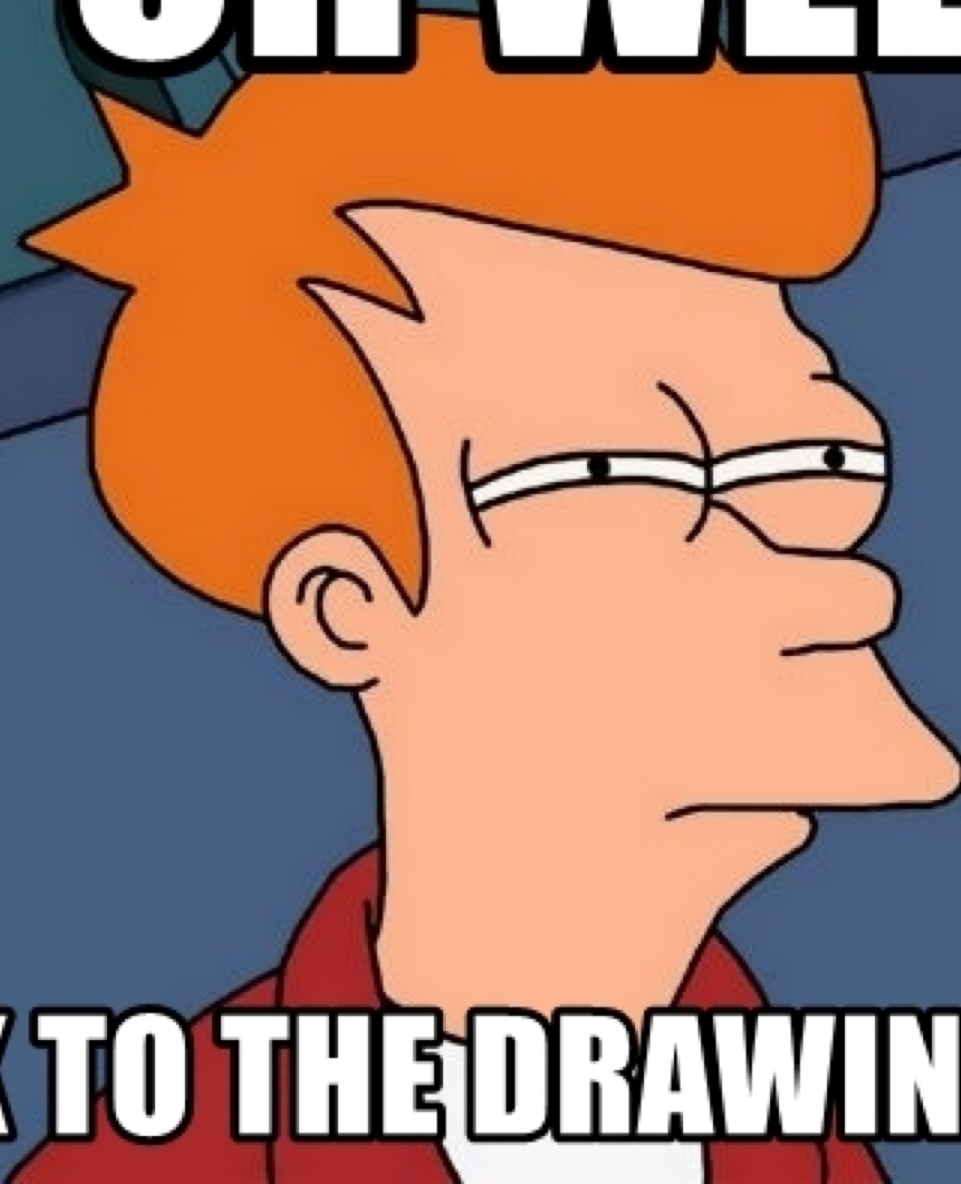
Testing Methodology

Manually explore all vendor built apps for data leakage???





OH WELL



BACK TO THE DRAWING BOARD

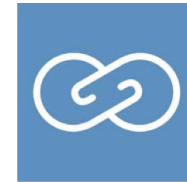
Testing Methodology

- Lets Try a Different Approach...
 - List vendors who build conference apps
 - Pick a few vendors and see if apps were leaking data
 - Automate testing for all apps by the vendor



Testing Methodology

- Some vendors that build conference apps



Testing Methodology

- The lucky vendors:
- Eventmobi
- Kitapps (Attendify)
- DoubleDutch



Another Disclaimer...!

I do not hold anything against these vendors

Testing Methodology

1. Manually check a few apps from each vendor to see if they leak sensitive info such as attendee PII
2. Find all apps built by the vendor
3. Automate the data extraction for all apps built by the vendor

Testing Methodology

1. Manually check a few apps by each vendor...

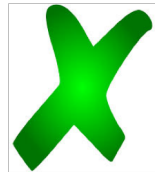
- Kitapps



- Eventmobi



- DoubleDutch



Testing Methodology

2. Find all apps built by the vendor

- Apple Appstore API?
- Android Appstore API?

Testing Methodology

- How do you find all apps built by a developer on the Android / iOS app stores?



Analytics Companies...!!!



eventmobi

See examples with OR and NOT clauses

Search in

Match style

☐ Description

☒ Contains

☒ Developer name

☐ Words Only

☒ Title

☐ Exact Match

STORE LISTING

☐ IDENTIFIER

☐ PUBLISHED STATUS

☐ GENRES

☐ IAB CATEGORIES

☐ CONTENT ADVISORY RATING

☐ DEVICE COMPATIBILITY

☐ RELEASED DATE

☐ UPDATED DATE

☐ AVAILABLE ON GOOGLE PLAY

☐ MORE LIKE THIS

☐ REVIEWS ANALYSIS

MONETIZATION

☐ PRICE

TECHNOLOGY INSIGHTS

☐ SDK INTEGRATIONS

DEVELOPER

☐ DEVELOPER NAME

☐ PHYSICAL ADDRESS

☐ WEB DOMAIN

1,418 apps match of 1,848,515

Export

TITLE	TRACK ID	DEVELOPER
EventMobi	1276348688	EventMobi
EventMobi 2017	1298239827	EventMobi
EventMobi Events	1220998757	EventMobi
EventMobi 2016	1071921699	EventMobi
EventMobi 2016	1122061636	EventMobi
EventMobi 2016	923401842	EventMobi
EventMobi 2016	946082757	EventMobi
EventMobi 2016	950780905	EventMobi
EventMobi 2016	992659270	EventMobi
EventMobi 2016	993315326	EventMobi
EventMobi 2016	1008293078	EventMobi
EventMobi 2016	1014073903	EventMobi
EventMobi 2016	1029166161	EventMobi
EventMobi 2016	1038149293	EventMobi
EventMobi 2016	1041468608	EventMobi
EventMobi 2016	1042802863	EventMobi
EventMobi 2016	1046116159	EventMobi
EventMobi 2016	1047823034	EventMobi
EventMobi 2016	1049880730	EventMobi
EventMobi 2016	1050437084	EventMobi

Double Dutch

See examples with OR and NOT clauses

Search in

Match style

☐ Description

☒ Contains

☒ Developer name

☐ Words Only

☒ Title

☐ Exact Match

STORE LISTING

☐ IDENTIFIER

☐ PUBLISHED STATUS

☐ GENRES

☐ IAB CATEGORIES

☐ CONTENT ADVISORY RATING

☐ DEVICE COMPATIBILITY

☐ RELEASED DATE

☐ UPDATED DATE

☐ AVAILABLE ON GOOGLE PLAY

☐ MORE LIKE THIS

☐ REVIEWS ANALYSIS

MONETIZATION

☐ PRICE

TECHNOLOGY INSIGHTS

☐ SDK INTEGRATIONS

DEVELOPER

☐ DEVELOPER NAME

☐ PHYSICAL ADDRESS

☐ WEB DOMAIN

1,155 apps match of 1,848,515

Export

TITLE	TRACK ID	DEVELOPER
Double Dutch Our Lives 2018	1360057679	DoubleDutch
Double Dutch Jump	1052308094	Double Dutch Ju...
Double Dutch Conferences	891911066	DoubleDutch
Double Dutch	553371956	DoubleDutch
Double Dutch USA Convention...	1035686357	DoubleDutch
Double Dutch	988177198	DoubleDutch
Double Dutch	869683981	DoubleDutch
Double Dutch Family Events	1114981057	DoubleDutch
Double Dutch International Air ...	1117318906	DoubleDutch
Double Dutch	467198066	DoubleDutch
Double Dutch	1242657632	DoubleDutch
Double Dutch	996119330	DoubleDutch
Double Dutch	892519751	DoubleDutch
Double Dutch	1196382099	DoubleDutch
Double Dutch	797190699	DoubleDutch
Double Dutch	974704768	DoubleDutch
Double Dutch	494119943	DoubleDutch
Double Dutch	497048413	DoubleDutch
Double Dutch	555068273	DoubleDutch
Double Dutch	580209613	DoubleDutch

kitapps

See examples with OR and NOT clauses

Search in

Match style

☐ Description

☒ Contains

☒ Developer name

☐ Words Only

☒ Title

☐ Exact Match

STORE LISTING

☐ IDENTIFIER

☐ PUBLISHED STATUS

☐ CATEGORIES

☐ IAB CATEGORIES

☐ FAMILY CATEGORIES

☐ CONTENT RATING

☐ PROMO VIDEO

☐ RELEASED DATE

☐ UPDATED DATE

☐ EDITORS' CHOICE

☐ AVAILABLE ON IOS APP STORE

☐ MORE LIKE THIS

☐ REVIEWS ANALYSIS

MONETIZATION

☐ PRICE

☐ IN-APP PURCHASES

☐ CONTAINS ADS

TECHNOLOGY INSIGHTS

☐ SDK INTEGRATIONS

☐ PERMISSIONS

806 apps match of 2,919,877

Export

TITLE	PACKAGE NAME	DEVELOPER
Attendify	com.attendify.app	KitApps, Inc.
Attendify: Winning Together	com.attendify.confhdc34	KitApps, Inc.
Attendify: Growing Together	com.attendify.confkuckpe	KitApps, Inc.
Attendify: Connect	com.attendify.confn3h9sq	KitApps, Inc.
Attendify: Group, Inc.	com.attendify.confkzpxzy	KitApps, Inc.
Attendify: Convention	com.attendify.saealumni...	KitApps, Inc.
Attendify: 2018	com.attendify.confliiziji	KitApps, Inc.
Attendify: Sports Tour	com.kitapps.android.buil...	KitApps, Inc.
Attendify: Tecnocasa México	com.attendify.confk0e9sd	KitApps, Inc.
Attendify: Sports Conference	com.attendify.conf6pomlr	KitApps, Inc.
Attendify: Pirates!	com.fwa.confj5mgp8	KitApps, Inc.
Attendify: N.A. Convention	com.attendify.app2014m...	KitApps, Inc.
Attendify: 2018	com.enactus.conf8zmc87	KitApps, Inc.
Attendify: Atlanta	com.attendify.conf69a6ai	KitApps, Inc.
Attendify: Con Nordics	com.attendify.confk7yyy	KitApps, Inc.
Attendify: Online ACCELERATE event	com.bpmonline.conf4v0...	KitApps, Inc.
Attendify: Ingeniería 2018	com.estrategia.confliq4d	KitApps, Inc.
Attendify: TechMeld 2018	com.ivpmpl.conf4p38qm	KitApps, Inc.
Attendify: Conclude	com.attendify.confbrsbuz	KitApps, Inc.
Attendify: IAS Convention 2018	com.icna.conf8iponr	KitApps, Inc.

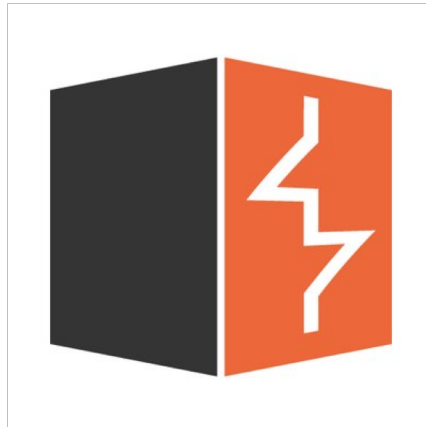
Testing Methodology

- Automated Data Extraction
 - Each vendor has a API schema
 - Same API must be used for all apps
 - Can I write a tool to parse through the API's for all the apps the vendor has to get all data being leaked???



Testing Methodology

- Browse the 'list attendees' feature for one app



List of API
endpoints for a
single app

Testing Methodology

- Tool to use the API to scrape all sensitive data for a single App.

Lets call that **Tool 1**

Testing Methodology

- How do you do this for all the apps ????
 - Same API's
 - Theoretically it should be doable
- What's different from one app to another???



Testing Methodology

- Compared burp logs for two apps from the same vendor
- Each app has a unique id
- Lets call this **app-id**



Testing Methodology

- Relation between the different id's ??
- Kitapps app-ids : db4xpj , yrgqgo
- Eventmobi app-ids : emciifall2016

(Was not always in this pattern)

Testing Methodology

- Finding the unique ID for individual apps..??



Testing Methodology

- Remember the online tools that had the list of apps developed by each vendor
- It has other interesting data in there too..



Testing Methodology

42-Matters 'package-id' and 'bundle-id'
contains the **app-id**



Applications ?

▶ Google Play

🍏 iOS App Store

👍 Popular Searches ▼

No saved queries yet

eventmobi

[See examples with OR and NOT clauses](#)

Search in

☐ Description

☒ Developer name

☒ Title

Match style

☒ Contains

☐ Words Only

☐ Exact Match

STORE LISTING

☐ IDENTIFIER

☐ PUBLISHED STATUS

☐ GENRES

☐ IAB CATEGORIES

☐ CONTENT ADVISORY RATING

☐ DEVICE COMPATIBILITY

☐ RELEASED DATE

☐ UPDATED DATE

☐ AVAILABLE ON GOOGLE PLAY





















1,407 apps match of 1,848,445

Export

📁 TITLE

📦 TRACK ID

📦 BUNDLE ID

<input type="checkbox"/>	 #Cinanz2016		1155113041	com.fivetouchsolutions.emciifall2016
<input type="checkbox"/>	 #CinanzLE2017		1209151101	com.fivetouchsolutions.emcmconference2017
<input type="checkbox"/>	 DFK 2016		1215321256	com.fivetouchsolutions.emdfk2017
<input type="checkbox"/>	 #Stoco		1153736253	com.fivetouchsolutions.emfstoco2016
<input type="checkbox"/>	 #Stoco		1294808024	com.fivetouchsolutions.emgitm17
<input type="checkbox"/>	 #HIVD16		1160811870	com.fivetouchsolutions.emhightechventuredays2016
<input type="checkbox"/>	 pf Berlin		1114027612	com.fivetouchsolutions.empfberlin
<input type="checkbox"/>	 pf Hamburg		1114032871	com.fivetouchsolutions.empfhamburg
<input type="checkbox"/>	 100Kin10 Summit		1221509585	com.fivetouchsolutions.em100kin10
<input type="checkbox"/>	 2016 Agent Convention		1158105442	com.fivetouchsolutions.em2016convention

Applications ?

▶ Google Play

iOS App Store

Popular Searches ▾

No saved queries yet

kitapps ?

[See examples with OR and NOT clauses](#)

Search in

☐ Description☒ Developer name☒ Title

Match style

☒ Contains☐ Words Only☐ Exact Match

STORE LISTING





















☐ IDENTIFIER ?☐ PUBLISHED STATUS ?☐ CATEGORIES ?☐ IAB CATEGORIES ?☐ FAMILY CATEGORIES ?☐ CONTENT RATING ?☐ PROMO VIDEO ?☐ RELEASED DATE ?☐ UPDATED DATE ?

809 apps match of 2,913,376

Export

TITLE

PACKAGE NAME

<input type="checkbox"/>	 Attendify		com.attendify.app
<input type="checkbox"/>	 Sephora Winning Toget...		com.attendify.confhgdc34
<input type="checkbox"/>	 Sephora Growing toge...		com.attendify.confxuckpe
<input type="checkbox"/>	 NTE Connect		com.attendify.confh3h9sq
<input type="checkbox"/>	 The SK Group, Inc.		com.attendify.confkzpxzy
<input type="checkbox"/>	 SAE Convention		com.attendify.saealumnicvention2014
<input type="checkbox"/>	 Unite 2018		com.attendify.confiiiznji
<input type="checkbox"/>	 Success Tour		com.kitapps.android.builder.brianbuffinissuccesstour
<input type="checkbox"/>	 Grupo Tecones México		com.attendify.confk0e9sd
<input type="checkbox"/>	 SETT Conference		com.attendify.conf6pomlr

Testing Methodology

- Another tool to extract app id's for all the apps built by a single vendor...
- Lets call this **Tool 2**

Testing Methodology

Tool2

Testing Methodology

- Getting all data exposed by a single vendor for all their apps

Tool2

Tool1

Testing Methodology

- Getting all data exposed by a single vendor for all their apps

Tool2 + Tool1 =



Findings

- Number of Attendees information available: ~500,000*
(combined kitapps and eventmobi)

Findings

- Types of data potentially exposed:
 - First Name
 - Last Name
 - Email
 - Phone Number
 - City/Country
 - Bio
 - Profile Pic {exif data from the images had not been scrubbed}*
 - LinkedIn URL
 - Twitter URL
 - Facebook URL

Findings

- EventMobi:
 - Total number of attendee PII available : ~230k
 - Total number of apps leaking data : ~550
 - Data from Top 10 apps : ~40k attendees



Findings

- <https://api.eventmobi.com/en/api/v1/events/<redacted>/sections/<redacted>/items/<redacted>>

This XML file does not appear to have any style information associated with it. The document tree is shown below.

```
<?xml>
<status>success</status>
<response>
  <id><redacted></id>
  <first_name><redacted>/first_name>
  <about/>
  <image50>
    50image_<redacted>.jpeg
  </image50>
  <image100>
    100image_<redacted>.jpeg
  </image100>
  <title>App-Admin</title>
  <company_name/>
  <threetopics/>
  <website/>
  <facebook>http://facebook.com/<redacted>/facebook>
  <twitter/>
  <linkedin/>
  <external_id><redacted></external_id>
  <custom_fields_values/>
  <attendee_agenda/>
  <url>
    https://api.eventmobi.com/en/api/v1/events/<redacted>/sections/<redacted>/items/<redacted>
  </url>
</response>
<timestamp>1551577035</timestamp>
</xml>
```


Findings

- Kitapps:
 - Total number of attendee PII available:~200k
 - Total number of apps leaking data:~700
 - Data from Top 10 apps : ~26k attendees



Findings

- <https://s3.amazonaws.com/kitapps.photo/<redacted>.jpg>



- QR code for attendees:

<https://qr.attendify.com/p/<redacted>?id=<redacted>&firstName=John&lastName=Doe>

Findings

- Are apps from previous years still available???
- There were apps from 2015/2016 as well
- Might be older apps too



Applications ?

Google Play

iOS App Store

Popular Searches ▾

No saved queries yet

2015 AND eventmobi ?

[See examples with OR and NOT clauses](#)

Search in

☐ Description☒ Developer name☒ Title

Match style

☒ Contains☐ Words Only☐ Exact Match

STORE LISTING

☐ IDENTIFIER ?☐ PUBLISHED STATUS ?☐ GENRES ?☐ IAB CATEGORIES ?

2 apps match of 1,848,445

Export

TITLE	TRACK ID	CONTACT	DEVELOPER
<input type="checkbox"/> [App Icon] 2015	10000000078	Show contacts	EventMobi
<input type="checkbox"/> [App Icon] Club2015	10000000054	Show contacts	EventMobi

Applications ?

Google Play

iOS App Store

Popular Searches ▾

No saved queries yet

kitapps AND 2016 ?

[See examples with OR and NOT clauses](#)

Search in

☐ Description☒ Developer name☒ Title

Match style





☒ Contains☐ Words Only☐ Exact Match

STORE LISTING

☐ IDENTIFIER ?☐ PUBLISHED STATUS ?☐ CATEGORIES ?☐ IAB CATEGORIES ?☐ FAMILY CATEGORIES ?☐ CONTENT RATING ?

2 apps match of 2,913,228

Export

	TITLE		PACKAGE ...	CATEGORY	DEVELOPER
<input type="checkbox"/>	 [REDACTED] 2016		com.attendify.c...	Business	KitApps, Inc.
<input type="checkbox"/>	 [REDACTED] 2016		com.attendify.c...	Business	KitApps, Inc.

Responsible Disclosure

- Reached out via email to the 2 vendors
 - Kitapps (Attendify)
 - Eventmobi
- Initial reach out around late Sept 2018



Responsible Disclosure

- Eventmobi product changes
 - Provide authentication feature free of cost
 - Require auth on all apps after 12 months of existence



Recommendations

- For Vendors building apps
 - Provide authentication at no extra cost
 - Remove apps after event completion
 - Recommend secure settings to your customers
 - Maintain a email where researchers can reach out to you



Recommendations

- If you use a vendor to build your apps
 - Review functionality from a security perspective
 - Use authentication
 - Do not leave the app open to anyone
 - Delete app after event has completed
 - Do not release the apps using your Appstore accounts



Recommendations

- If you are an attendee going to a conference
 - Be cautious of the information you are putting in ~~a conference app~~ any app really
 - Do not connect LinkedIn/Twitter/Facebook
 - Check scopes of OAuth connected apps
 - Remove app connections when you can



Open Questions

- Who owns these apps???
 - Developer
 - Customer for whom the developer built the app
- Why are so many apps open?
 - Maybe authentication means more \$\$\$
 - Convenience



Future Work

- Expanding this to more developers/vendors
- Search for more stats on number of cons and how they are categorized on the app stores
- Any other ideas?

Any Questions...
Just Ask!

